DETAILED ACTION

In view of the appeal brief filed on 09/30/2009, PROSECUTION IS HEREBY REOPENED. New grounds of rejections are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 13 – 16, and 18 - 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani et al. (US 6,393,484), in view of Larson et al. (US 2004/0107286)

Regarding claims 13 and 18, Sitaraman et al. teaches a method in an IP network, the network including a switch node, **[Fig. 1, Ref # 26],**

at least one DHCP server, **[Fig. 1, Ref # 30],**

and at least one subscriber being associated with the node, **[Fig. 1, Ref # 12 shows dynamic end users],**

transmitting by the subscriber a DHCP request message for an IP address, **[the end user device such as a PC or CM will initiate a DHCP exchange in an attempt to obtain a valid IP address and other associated parameters, as shown in Fig. 4, Ref # 404, (Massarani et al., Col. 6, lines 25 – 30)],**

receiving a reply message which carries an assigned subscriber IP address, **[the DHCP server will process the end user's device DHCP request and extract the end**

user's device MAC address from the database 32, as shown in Fig. 4, Ref # 408, (Massarani et al., Col. 6, lines 35 – 40)],

analyzing the reply message to be a DHCP message and having a source address from one of the trusted DHCP servers, **[A test 410 is performed to determine whether the MAC address is registered, If the MAC address is valid, that is belongs to a registered user, a "yes" condition for the test 410 activates the DHCP server in an operation 414, selects an appropriate IP address and associated parameters to be returned to the requesting end user device, as shown in Fig. 4, (Massarani et al., Col. 6, lines 40 - 53)],**

updating a filter dynamically in the node, the filter storing an identification of the subscriber and the assigned subscriber IP address, **[the DHCP server dynamically sets up filter rules in the router switch limiting access to a subset of IP addresses such as the address of a log-in server. DHCP processing is completed and an IP address is assigned to the requesting end user's device by DHCP, (Massarani et al., Col. 3, lines 50 - 60)],**

transmitting a frame from the subscriber device using a source IP address, **[an operation 422 is performed to send the DHCP response to the device with the IP address and other parameters, after which the process ends as shown in Fig. 4, wherein the frame includes the sent IP address, (Massarani et al., Col. 7, lines 34 – 38)],**

comparing in the filter said source IP address with the stored subscriber IP address, **[An operation 310 scans the DHCP table for unregistered entries as**

shown in Fig. 3, wherein the filter compares the IP addresses, (Massarani et al., Col. 6, lines 15 – 22)],

discarding said frame when said source IP address differs from the stored subscriber IP address, **[invalidates ARP entries and provides a log/alert if any are found and transfers to the operation 306 after disabling of the ARP the configuration operation terminates, wherein the disabling of the ARP refers to discarding the frame that includes the IP address, , (Massarani et al., Col. 6, lines 15 – 23)],**

Massarani et al. fails to explicitly teach creating a list of trusted ones of the DHCP servers,

Larson et al. teaches a secure mechanism for communicating over the internet employs a number of special routers or servers, **(Larson et al., Paragraph 70)**, in order to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN, **(Larson et al., Paragraph 8),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Massarani et al. by creating a list of trusted ones of the DHCP servers, **(Larson et al., Paragraph 70)**, in order to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN, **(Larson et al., Paragraph 8).**

Regarding claim 14, the method in an IP network according to claim 13, further comprising the step of storing in the filter a subscriber MAC address, a subscriber physical port number, and a lease time interval for the assigned subscriber IP address, **[storing in the database user/device registration information including a Medium Access Control (MAC) address, (Massarani et al., Claim 1)].**

Regarding claim 15, the method in an IP network according to claim 13, wherein the subscriber IP address is statically assigned and handled by the DHCP servers, **[shared network access ports work in conjunction with Dynamic Host Control Protocol (DHCP) servers to dynamically assign the appropriate IP address and other parameters to a mobile employee's device, (Massarani et al., Col. 1, lines 22 – 26)].**

Regarding claim 16, the method in an IP network according to claim 14, the method including deleting the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval is out, **[if the DHCP lease expires in an operation 601, the DHCP server will invalidate the corresponding ARP IP to MAC table entry in the associated router/switch and reset any IP permissive IP filtering for the device in an operation 603, (Massarani et al., Col. 7, lines 10 – 15)].**

Regarding claim 19, the device in an IP network according to claim 18, the device being further operative to store in the filter a subscriber MAC address, a subscriber physical port number, a subscriber virtual LAN identity, and a lease time interval for the assigned subscriber IP address, **[storing in the database user/device registration information including a Medium Access Control (MAC) address, (Massarani et al., Claim 1)].**

Regarding claim 20, the device in an IP network according to claim 18, wherein the subscriber IP address comprises a statically assigned address which is handled by the DHCP servers, **[shared network access ports work in conjunction with Dynamic Host Control Protocol (DHCP) servers to dynamically assign the appropriate IP address and other parameters to a mobile employee's device, (Massarani et al., Col. 1, lines 22 – 26)].**

Regarding claim 21, the device in an IP network according to claim 19, the device being further operative to delete the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval is out, **[if the DHCP lease expires in an operation 601, the DHCP server will invalidate the corresponding ARP IP to MAC table entry in the associated router/switch and reset any IP permissive IP filtering for the device in an operation 603, (Massarani et al., Col. 7, lines 10 – 15)].**

Claims 17 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani et al. (US 6,393,484), in view of Larson et al. (US 2004/0107286) and further in view of Taylor et al. (US 2002/0065919).

Regarding claims 17 and 22, The modified Massarani et al. teaches the method in an IP network according to claim 13, the method further comprising the steps of: counting a number of attempts (n) from the subscriber to use an illegitimate IP address, **[In FIG. 4 the end user device such as a PC or CM will initiate a DHCP exchange in an attempt to obtain a valid IP address and other associated parameters, (Massarani et al., Col. 6, lines 25 – 30)],**

The modified Massarani et al. fails to teach sending a warning signal when the number of attempts exceeds a threshold criteria,

Taylor et al teaches comparing the number (n) of the attempts with a threshold number (N), **[DB servers may include circuitry which checks for a time stamp discrepancy which exceeds a particular threshold, and sends a warning message, wherein the numbers are compared with a specific threshold, (Taylor et al., Paragraph 131)],**

Taylor et al further teaches sending a warning signal when the number of attempts exceeds a threshold criteria, **(Taylor et al., Paragraph 131, Page 8)**, in order to increase security, **(Taylor et al., Paragraph 167, Page 10)**,

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Massarani et al. by comparing the number (n) of the attempts with a threshold number (N), DB servers may include circuitry which checks for a time stamp discrepancy which exceeds a particular threshold, and sends a warning message, wherein the numbers are compared with a specific threshold, **(Taylor et al., Paragraph 131, Page 8),** and sending a warning signal when the number of attempts exceeds a threshold criteria, **(Taylor et al., Paragraph 131, Page 8)**, in order to increase security, **(Taylor et al., Paragraph 167, Page 10)**.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Shaq Taha** whose telephone number is 571-270-1921. The examiner can normally be reached on 8:30am-5pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Jeff Pwu** can be reached on 571-272-6798.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/S. T./

Examiner, Art Unit 2446

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446